Notice of Allowability	Application No.	Applicant(s)	
	09/756,346	HAVERINEN ET AL.	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *after-final amendment of 3/29/2006*.

2. ☒ The allowed claim(s) is/are *1-10,12,15,23,25 and 26*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

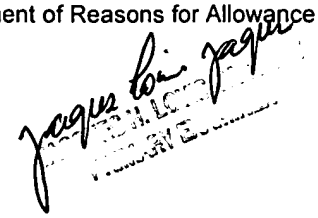
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.



DETAILED ACTION

1. The response of 3/29/2006 was received and considered.

2. Claims 1-10, 12, 15, 23 & 25-26 are pending.

3. An Examiner's amendment appears on p. 3.

4. The Examiner's reasons for allowance appear on p. 4.

5. As per the Examiner's amendment, claims 1-10, 12, 15, 23 & 25-26 are allowed.

EXAMINER'S AMENDMENT

6. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Geza Ziegler on 4/7/2006.

The application has been amended as follows:

1. In claim 15, line 3, please replace "the gateway" with "the network entity" such that line 3 of claim 15 reads "**server, the network entity comprising:**".

2. Please cancel claim 14.

3. Please cancel claim 16.

4. Please cancel claim 21.

Allowable Subject Matter

6. Claims 1-10, 12, 15, 23 & 25-26 are allowed.

7. The following is an examiner's statement of reasons for allowance:

Federrath discloses providing the mobile node/station with a mobile node identity/TMSI and a shared secret/Ki specific to the mobile node identity/TMSI and usable by a telecommunications network/home network (Fig. 1, p. 5), sending the mobile node identity/TMSI from the mobile node to the network/visited network, providing the network/visited network with authentication information usable by the telecommunications network/home network, the authentication information comprising a challenge/RAND and a session secret/Kc corresponding to the mobile node identity/TMSI and derivable using the challenge/RAND and the shared secret/Kc (Fig. 1, p. 5), sending the challenge/RAND from the network/visited network to the mobile node/station (Fig. 1, p. 5), generating at the mobile node the session secret/Kc and a first response corresponding/SRES to the challenge/RAND, based on the shared secret/Ki (Fig. 1, p. 5), sending the first response/SRES to the packet data network, and checking/authenticating the first response for authenticating the mobile node (Fig. 1, p. 5). **Sayers** teaches that to as wireless technology becomes more popular, companies desire to let workers increase mobility and access all voice and data information via wireless networks (col. 6, lines 58-65). Sayer's system comprises a private wireless network (Fig. 2) where mobile stations/phones communicate with protocol converters (P-BTS) that communicate with an IP network, such as the Internet (Fig. 2, #24) through a protocol interface (Fig. 2, #28-1) (see also col. 9, lines 26-65). Further, Sayers teaches that the software of the P-BTSs provide support for call connection in the wired protocol (col. 10, lines 49-62). **Menezes** teaches that random

numbers can be used in challenge-response mechanisms to provide timeliness assurances and avoid certain replay and interleaving attacks (§10.3.1 (i)). Menezes teaches that nonces can be used to provide timeliness guarantees where a receiving party (network) creates a response (cryptographic information) that depends both on a secret/Kc and the challenge/nonce (protection code) (§10.3 & §10.3.1 Background). **Abrol** teaches that by using a data service node/gateway that supports authentication between a mobile node and an authentication server, the benefit of providing authentication for a diverse set of mobile stations in a wireless network is gained (p. 3, ¶2-3). The data service node/gateway performs authentication techniques for the mobile station; otherwise, an authentication server is accessed (p. 3, ¶2).

However, regarding claim 1, the prior art relied upon fails to teach or suggest the challenge being based on RAND codes of at least two authentication triplets of the telecommunications network, in combination with the other elements of the claim; and

Regarding claim 15, the prior art relied upon fails to teach or suggest receiving at least two challenges corresponding to the mobile node identity from the authentication server, forming cryptographic information based on the at least two received challenges and to output the two received challenges and the cryptographic information for transmission to the mobile node, in combination with the other elements of the claim.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis Jacques can be reached at (571) 272-6962.

Any response to this action should be mailed to:
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(571) 273-8300
(for formal communications intended for entry)
Or:
(571) 273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS

April 6, 2006